UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/941,898	08/29/2001	Hideaki Watanabe	09792909-5125	7578

26263 7590 10/27/2005

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/941,898	WATANABE ET AL.	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1,11,20, and 22 have been amended.

2. Claims 1-22 are pending.

Response to Arguments

1. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection, Khidekel et al. (Pub No. 2001/0027527)

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Musgrave et al. (US Patent No. 6,505,193) in view of Khidekel et al. (Pub No. 2001/0027527). As per claims 1,11,22, and 22, Musgrave et al. discloses a public-key certificate using method, system, and program for using a public key certificate which functions, in association with digital signature data of a certificate authority, comprising: a person identification certificate authority which execute a person authentication by comparing sampling information which serves as person identification data of a person requesting a public key certificate against a template which serves a person identification data of the person requesting a public key certificate, being obtained from a person identification, and a certificate authority which issues a public key certificate

for the requesting person on condition that the person authentication is established. (See Column 5, lines 38-67, Column 6, lines 1-9)

However, Musgrave et al. fails to explicitly disclose an identification request device for generating a pair of the public key and a private key for a user who inputs sampling information that serves as person identification data of a person requesting the public key certificate, and sending the public key, the private key, and the sampling information to a person identification certificate authority.

Khidekel et al. discloses a secure communication system wherein a user identification request is submitted for generating a digital certificate. The user inputs sampling information such as fingerprint data. The certificate authority verifies that the identification information, creating a user certificate and binds the certificate with authentication information such as shared (private/public key pair) and the sampling information such as fingerprint data. The information is stored within an authentication device and the certificate is returned to the user. (See pages 2-3, Sections 0028-0031)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Musgrave et al.'s system and method for biometric databases by combining Khidekel et al.'s secure transaction system. The teaching of this combination will enable secure communication over a public network and validate digital signatures within a public key certificate system. (See Khidekel et al., page 1, Section 0004)

As per claims 2 and 12, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein the person identification

certificate authority obtains sampling information which serves as person identification data of the person requesting a public key certificate, executes a person authentication by comparing the sampling information against a template obtained from the person identification certificate, and notifies the certificate authority of a success of the person authentication, issuing a public key certificate for the requesting person in response. (See Column 6, lines 10-45)

As per claims 3 and 13, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein the person identification certificate authority executes a mutual authentication with the certificate authority on condition that the person authentication is established on the basis of the person identification certificate of the person requesting a public key certificate, and transmits a public key of the person requesting a public key certificate to the certificate authority on condition that the mutual authentication is established, the certificate authority issuing a public key certificate associated with the public key received. (See Column 5, lines 61-67, Column 6, lines 1-9)

As per claims 4 and 14, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein the public key certificate issued by the certificate authority is a one-time public key certificate which is effective only for a single processing session involving use of an associated public key, based on the person authentication on the basis of the person identification certificate. (See Column 17, lines 12-41)

As per claims 5 and 15, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein each of the person identification certificate authority and the certificate authority is implemented by a third party which is not in association with a user of the public key certificate and the person identification certificate. (See Column 15, lines 7-21, Column 17, lines 42-48)

As per claims 6 and 16, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein the person authentication is executed on the basis of user-entered sampling information transmitted from the authentication requesting device to the person identification certificate authority, the transmission of the user-entered sampling information being executed on condition that a mutual authentication is established between the authentication requesting device and the person identification certificate authority. (See Column 9, lines 18-67, Column 10, lines 1-7)

As per claims 7 and 17, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein the user device transmits user-entered sampling information to the person identification certificate authority, the person identification certificate authority executes the person authentication by comparing the sampling identification against the template obtained from the person identification certificate, the certificate authority issues a public key certificate the user to the user device on condition that the person authentication is established. (See Column 13, lines 44-67, Column 14, lines 1-26)

As per claims 8 and 18, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method and system wherein the certificate authority issues the public key certificate to the user device, the public key certificate being stored in the storage, and the user device deletes the public key certificate upon completion of a processing session. (See Column 16, lines 24-65)

As per claims 9,19, and 21, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using method, system and program wherein the certificate authority issues the public key certificate to the user device, the public key being stored in the storage, the user device deletes the public key certificate, and a public key and a private key is stored upon completion of a processing session. (See Column 17, lines 27-50)

As per claim 10, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using system wherein the template comprises personal biometric information such as fingerprint, retina pattern, iris pattern, voiceprint, and handwriting information, non-biometric information such as a seal, a passport, a driver's license, and a card, any combination of the two or more biometrics with a password. (See Column 17, lines 42-67, Column 18, lines 1-3)

As per claim 20, (Musgrave et al. as modified by Khidekel et al.) discloses a public-key certificate using apparatus comprising: means for receiving a public key certificate which is issued to a user on condition that a person authentication is established by a person identification certificate authority by comparing sampling information of a user against a template, means for storing the public key, and means

for deleting the public key upon completion of a processing session. (See Column 18, lines 37-52)

However, Musgrave et al. fails to explicitly disclose an identification request device for generating a pair of the public key and a private key for a user who inputs sampling information that serves as person identification data of a person requesting the public key certificate, and sending the public key, the private key, and the sampling information to a person identification certificate authority.

Khidekel et al. discloses a secure communication system wherein a user identification request is submitted for generating a digital certificate. The user inputs sampling information such as fingerprint data. The certificate authority verifies that the identification information, creating a user certificate and binds the certificate with authentication information such as shared (private/public key pair) and the sampling information such as fingerprint data. The information is stored within an authentication device and the certificate is returned to the user. (See pages 2-3, Sections 0028-0031)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Musgrave et al.'s system and method for biometric databases by combining Khidekel et al.'s secure transaction system. The teaching of this combination will enable secure communication over a public network and validate digital signatures within a public key certificate system. (See Khidekel et al., page 1, Section 0004)

Conclusion

2. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
October 20, 2005

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER